FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer & Business Education

Holiday Shopping Online:
Plan Ahead for Secure Surfing

With the holidays fast approaching, online shopping is a great way to get a jump on getting all your gifts. But the Federal Trade Commission (FTC) — the nation's consumer protection agency — says that before starting to shop on the Internet, consumers should know how to keep their computer and private information secure. The FTC encourages online shoppers to follow these tips to be sure that no online grinch or gremlin gets in the way of their celebration.

- **Use anti-virus software and a personal firewall and keep them up-to-date.** Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that: recognizes current viruses as well as older ones; can effectively reverse any damage; and updates automatically. Make sure that you update your anti-virus protection software regularly. A firewall blocks unauthorized access to your computer; if you have a broadband connection, it's especially important that you run a firewall to block communications from unauthorized sources.

- **Make sure your web browser and operating system are up-to-date.** Your web browser security setting should be high enough to detect unauthorized downloads, for example, at least the "Medium" setting for Internet Explorer. Your operating system (like Windows or Linux) may offer free software "patches" to close holes in the web browser or operating system that spyware, hackers, or phishers could exploit.

- **Don't email your financial information.** Email is not a secure method of transmitting financial information like your credit card, checking account, or Social Security number. If you initiate a transaction and want to provide your financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some fraudulent sites have forged security icons.

- **Be cautious about opening any attachment.** Don't open an email attachment — even if it looks like it's from a friend or co-worker — unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining what it is. Remember not to click on links in pop-up ads. They could install harmful files on your computer.

For more information about protecting your computer and your personal information online, visit www.ftc.gov/infosecurity.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.